# Behind The Mystery Of Russia's 'Dyre' Hackers Who Stole Millions From American Business

forbes.com/sites/thomasbrewster/2017/05/04/dyre-hackers-stealing-millions-from-american-coporates

Thomas Brewster May 4, 2017


This article is more than 5 years old.

Paint maker and retailer Sherwin-Williams Company was a victim of one of Russia's most active cyber... [+] gangs in 2014, according to a search warrant. (AP Photo/Pat Wellenbach)

Around Halloween 2014, Ohio-based building materials and paint company Sherwin-Williams got an expensive scare - a cyberattack. Seven suspect wires worth around $6.45 million were sent from its French subsidiary's corporate account at Morgan Chase to organizations across China, Latvia, Liechtenstein and the Netherlands between October 27 and 30. They were not legitimate transactions. And those organizations were being used as part of a huge illegal operation.

This is according to a just-unsealed search warrant unearthed by *Forbes*, which revealed the $30 billion-valued Sherwin-Williams was hit by one of the Russia's most successful criminal gangs, known as Dyre. A source with knowledge of the fraudulent transfers confirmed the facts outlined in the FBI warrant.

It seemed that the Dyre crew's rapid rise to prominence was curtailed in late 2015, when Russia's FSB made multiple arrests of individuals suspected of being part of the group. Now sources say the hackers are likely active again with Trickbot, new but remarkably similar malware. Those sources also tell *Forbes* they believe many of those arrested for the multi-million criminal operation were released without being charged. And those allegations have only intensified fears that the Russian government does little to stop hackers carrying out costly cyberattacks against foreign businesses.

**The rise, demise and rebirth of Dyre**

For Sherwin-Williams, which boasts annual revenues of circa $10 billion, the cyber heist was pocket change. But it was a significant coup for Dyre, also the name of its own brand of banking malware that replaced infected victims' bank login pages with an imitation website to steal account passwords. According to the search warrant, unsealed in April by an Ohio court, Dyre swindled another major Ohio-based organization, Miba Bearings US, robbing the engine parts manufacturer of $4.8 million, its money transferred to bank accounts in China and Hong Kong. Sherwin-Williams declined to comment. Miba acknowledged Forbes' emails but hadn't provided comment at the time of publication. Neither had previously disclosed the breaches.

A phishing email containing the Dyre malware, designed to steal bank logins.
PhishMe

Miba and Sherwin-Williams are just two of many victims. At its height, Dyre was the most active financial malware on the web, stealing tens of millions from firms across America, the U.K. and Australia. Another major victim was the budget airline RyanAir, which was reportedly robbed of $5.5 million. By the time Sherwin-Williams was hacked, not long after Dyre first appeared in mid-2014, 45,000 U.S.-based PCs were infected with the group's malware (also known as Dyreza), out of a worldwide total of 133,000, according to the warrant.

The scope of the operation was extraordinary in both its aggressive expansion and its profitability. To dupe companies, the Dyre attackers used some particularly aggressive tactics. Where the target didn't enter their banking passwords into the fake web page, the hackers would call them directly over Skype, pretending to be the bank and encouraging them to hand over login information. On at least one occasion, according to the search warrant, a Dyre agent pretended to be a law enforcement officer.

A configuration file for Dyre showed the criminals created as many as 1,100 phishing websites, imitating login pages for all major Western banks, from Goldman Sachs to Wells Fargo to the Royal Bank of Scotland. They also went after customers of major platforms like Salesforce, which holds financial information such as payrolls.

Dyre topped the list for most active bank malware in 2015, but has been out of action since 18... [+]
November that year.
IBM

The Dyre crooks ran a huge network of “money mules” -- individuals and businesses that funnel funds from stolen victims through various bank accounts in a bid to prevent law enforcement from following the money back to the gang leaders. Dyre’s mules were situated in China, Hong Kong, The Netherlands and Latvia to name a few, according to the warrant. But they weren’t just employed to move money through financial institutions. They also laundered pilfered funds by purchasing Apple products, games consoles and military equipment to be resold within Russia for an amount higher than their commercial retail price, according to Brett Stone-Gross, e-crime analyst at CrowdStrike. They included MacBooks, iPads, PS4s, Xbox consoles, Roomba robot vacuums, guitars, rifle scopes and laser sights.

The whole operation came crumbling down in November 2015 when a Moscow-based film company, 25th Floor, was raided and arrests made. But there’s little information on just what role, if any, 25th Floor employees played in the Dyre conspiracy. Adding intrigue to the Dyre tale was the fact that 25th Floor was producing a film called Botnet, a thriller loosely based on a 2010 case involving a $3 million cybercrime. According to a source with knowledge of the FSB investigation, as many as 50 arrests were made during that raid, but most were released. *Forbes* could not independently verify that claim. 25th Floor CEO Nikolay Volchkov, who didn’t appear to be amongst those apprehended at the time, did not respond to requests for comment.

Global law enforcement agencies have continued to dismantle the campaign’s mule infrastructure, as the FBI warrant, dated September 2016, attests. In November, U.K. police arrested 14 individuals involved in a money mule group that laundered $14.2 million for Dyre and another notable cybercriminal operation called Dridex.

**The ghost of Dyre lives**

Much mystery remains about Dyre’s leaders. No names were ever released and no public charges revealed by Russian police. Sources with knowledge of the hackers’ activities say they believe some or all of the original gang members are still perpetrating cybercrimes. And not long after Dyre died, TrickBot was born. Its code contains notable similarities to Dyre’s eponymous malware and does much the same, imitating bank logins. Thus far it's been targeting major financial bodies in Australia and the U.K., including ANZ, HSBC and Lloyds Bank, according to configuration files for the malware.

It's yet to target U.S. organizations on the same scale as Dyre did, but IBM executive security advisor Limor Kessem believes it's a matter of time before TrickBot goes big. This month, the malware went from carrying out one to three major attacks per month, up to five, according to IBM data released in April.

Though there's no clear evidence linking the Dyre overlords with those behind TrickBot, the technical clues indicate they're the same, according to security experts and an FBI official, who asked to remain anonymous as he was not authorized to talk publicly on the subject. "I do suspect that TrickBot was not created by a new team, and that at least parts of the old Dyre team is involved in its development and operation," added Kessem.

Evgeniy Bogachev is one of the FBI's Most Wanted and found his way onto American sanctions of... [+] Russian individuals and entities following the U.S. election hacks of 2016. Dyre is linked to his alleged cybercrime operation, The Business Club, which has been tied to espionage activity.
Department of Justice

Dyre has also been linked to one of the world's biggest cybercrime gangs: the Business Club, a sprawling operation headed up by FBI Most Wanted, Evgeniy Bogachev. An indictment from May 2014 claimed he'd stolen as much as $100 million through cyberattacks with the Gameover Zeus banking malware and the Cryptolocker ransomware.

"We assess that [Dyre] is some or all of the same people including Bogachev," said SecureWorks analyst Alex Tilley. He pointed to technical links, including the use of a downloader tool called Upatre, used by both Dyre and Gameover Zeus, while noting some intriguing timing: "The timing is crucial from a technical point of view: the GameOver Zeus takedown was in June 2014 and after a few attempts at regaining control of the malware it goes quiet. Then two weeks later Dyre appears and it's going after the same target sector as GameOver Zeus and is using the same types of web injects… the facts don't point at any other group being setup to attack the same targets, using the same methods and evolutions of the same malware/tooling at that time."

Going further down the rabbit hole, the Business Club has been linked to Kremlin-backed spy operations too. In 2015, Forbes revealed Bogachev was also tied by security firms SecureWorks and CrowdStrike to Russian cyberespionage on foreign targets, including some in the U.S. The Russian government has previously denied any involvement in recruiting criminals to carry out cyberespionage.

**Kremlin-backed cybercrime?**

If, as sources say, some of the key Dyre operators are continuing to profit from cybercrime, even after the initial arrests, Western experts fear Russian agencies are backing hackers who target the U.S. and other nations, without stealing from the homeland. Bogachev is living freely in a city on the Red Sea, despite the accusations levelled at him, and is yet to stand trial anywhere. And alleged Yahoo hacker Alexsey Belan, who was accused by the U.S. of attacking other U.S.-based companies including Amazon and Evernote, was said by American prosecutors to have been encouraged by FSB agents. Neither Bogachev nor Belan could be contacted for comment.

It's this kind of alleged collusion that political and cyber experts have long suspected, but without any official claims until the Yahoo breach indictments hit in February, two months after both Belan and Bogachev appeared on the White House's sanctions on Russian entities in response to the cyberattacks on the 2016 election.

Neither of the two men could be reached for comment. The Kremlin, for its part, has denied any involvement in either the Yahoo or the election attacks.

But James Lewis, an intelligence and security specialist at the Center for Strategic and International Studies, said any digital thief residing in Russia simply has to follow some simple rules if they want to live a life of crime and remain free. "You can't operate in Russia unless you do what the government asks. There are three rules for Russian cybercriminals. Number one, don't hack in Russia - I'm now told it's don't hack Cyrillic language targets. Number two, share the wealth with the local FSB. Number three, if they ask you to do a favor, do it - e.g. act as a proxy force for the Russian state.

"Follow these and you'll never go to jail."